Published in Proceedings of the 1st International Workshop on Security and Communication Networks (IWSCN), 2009,
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5683061

A secure MANET routing protocol for first responders

Åsmund Ahlmann Nyre, Martin Gilje Jaatun, Inger Anne Tøndel
SINTEF ICT
Trondheim, Norway
Asmund.A.Nyre@sintef.no

Abstract

Emergency and rescue operations are often carried out in areas where the network infrastructure cannot be relied on for message exchange between first responders. Since the fundamental feature of a Mobile Ad Hoc Network is the ability to operate independently of existing infrastructure, it is deemed a well suited solution for first responder scenarios. In this paper we describe a security extension to the OLSR routing protocol specifically designed for first responder scenarios. Our proposed protocol provides node authentication and access control using asymmetric encryption and digital certificates. A link encryption scheme is devised to allow for efficient encryption of data even in broadcast mode, without the need for a network wide shared key. By utilising pairwise symmetric keys for link confidentiality, our solution is both efficient and scalable.

1. Introduction

Emergency and rescue operations are often carried out in areas where the network infrastructure cannot be relied on for message exchange between first responders. Although it may be argued that some network infrastructure (e.g. GSM/GPRS/UMTS, WiFi, WiMax, Satellite, etc.) exists in even the most deserted places, the cause of the emergency operation (e.g. fire, hurricane, explosion, etc.) may also affect the infrastructure. Additionally, rural infrastructure may not have been dimensioned for the network load imposed by a large-scale emergency operation. Since the fundamental feature of a Mobile Ad Hoc Network is the ability to operate independently of existing infrastructure, it is deemed a well suited solution for first responder scenarios.

The nature of emergency and rescue operations imply that providing information security is a prerequisite for MANETs to be used in such situations [1]. Unlike the general purpose MANET, a first responder MANET must restrict access to the network such that valuable resources (e.g. bandwidth, battery lifetime, processing power, etc.) are not wasted on activities not related to the operation. Access control also enables node authentication and confidentiality of information by only allowing authorised nodes to send and receive information. With limited resources and a great emphasis on availability, it is equally important that security mechanisms do not substantially affect the overall performance and throughput of the network.

Our main contribution in this paper is the design and specification of a new security extension to the Optimised Link State Routing (OLSR) protocol specifically tailored to first responder scenarios. Our protocol extension utilises digital certificates and asymmetric encryption for node authentication and symmetric key establishment. We also specify a new certificate extension to allow for distributed access control based on authorised node descriptions. To efficiently provide confidentiality, our protocol extension also includes a link encryption scheme utilising dynamically established symmetric keys between neighbouring nodes. By limiting the use of asymmetric encryption, our protocol extension is efficient.

This paper presents results from the OASIS[1] research project [2], [3]. We start by giving an overview of relevant state of the art on MANET security (Section 2). Next we present an overview of our proposed protocol extension in Section 3, before we detail our solution in Section 4. Finally we discuss our contribution (Section 5) before concluding and outlining further work in Section 6.

2. Related work

The standard protocols proposed for use in MANETs (e.g OLSR [4], AODV [5]) do not address the security of routing information, allowing a rouge node to easily launch attacks to disrupt routing, partition a network, or create black holes to thwart any communication [6]. However, there exists several extensions to these protocols that can be used to protect routing in ad hoc networks. Below we present a brief overview of such efforts.

Venkatraman et al. [7] suggest to use digital signatures to perform entity and message authentication related to routing information. In their approach, signatures creates a binding between the messages and the owner of the key, leaving adversaries unable to change, forge or replay any topology changes or routing table updates. To achieve this they require the establishment of a Public Key Infrastructure (PKI) with a trusted certificate authority that issues digital certificates [8] to the participating nodes prior to network deployment. The

1. Open Advanced System for dISaster and emergency management

problem of issuing and distributing Certificate Revocation Lists (CRLs) [8] is however not considered.

A similar approach is Authenticated Routing for Ad hoc Networks (ARAN) [9]; a signature-based extension to the AODV routing protocol providing secure route discovery. A route request is signed by the originator of the request, and intermediate nodes will check this signature before signing the request themselves and forwarding it to their neighbours. The ARAN protocol has been validated through a proof-of-concept implementation, and tests performed on this implementation suggest that the protocol increases the delay for route setup by several orders of magnitude. Even with fairly powerful laptops, the ARAN protocol using 1024 bits RSA keys is approximately 23 times slower than the unsecured AODV protocol [9]. The aim of reducing this computational overhead has lead to the development of the Secure AODV routing protocol (SAODV) [10]. This protocol introduces hash-chains for hop count authentication, thereby reducing the overhead at each intermediate node. For proactive link state protocols Secure Link State Protocol (SLSP) [11] employs a similar strategy as SAODV, using signatures for non-mutable data and hash chains for mutable data to secure the propagation of topology change messages. The use of a pre-configured maximum hop count, allows SLSP to be used as the proactive part of ZRP.

To further reduce the computational overhead protocols such as Ariadne [12] and the Secure Routing Protocol (SRP) [13] relies solely on symmetric key cryptography and hash chains for authenticated route discovery. However, both protocols assume that a shared secret has already been established between the source and destination and do not attempt to solve the problem of key agreement.

Several efforts have also been made to secure the forwarding of data traffic in MANETs. The Secure Transmission Protocol (STP) [14] utilises symmetric key encryption for reliable end to end authentication of data transmission. Messages are split up and sent on disjoint routes. Any missing packet will cause a resending and an update to the routing table by removing the failed route. Symmetric keys are assumed to be established in advance.

As pairwise shared secrets do not scale well, Puzar et al. [15] suggest a solution where every node in the network share the same key. Mechanisms are defined that result in the key to change at times, but during key re-selection the network is in an inconsistent state unable to route messages. Because of the problems with network wide keys, we do not believe this to be the best solution for MANETs. Still Puzar et al. specifically address emergency and rescue operations, and many of their ideas fit well within this setting; they rely on pre-existing certificates to be in place, all certificates are signed by the same CA, and they put restrictions on which nodes are authorised to influence routing.

3. Protocol overview

In this section we outline the main features of our proposed protocol. We first provide a brief overview of first responder characteristics and requirements, before providing a basic overview of the OLSR protocol for MANETs, which we base our specification on. Next we describe how a certificate hierarchy is assumed organised and the authentication and access control procedure is accomplished. Finally we give a brief description of our link encryption scheme.

3.1. First responder characteristics and requirements

While MANETs in the general case should allow anyone to participate, the situation is quite the contrary for first responders. First responders require an access control that prevents nodes from wasting their resources (energy, processing power, bandwidth, etc.) on information that is not relevant for the mission. While this normally requires preconfiguration, the mechanism should be flexible enough to allow temporary access to nodes that have not been preconfigured. This will allow first responders to dynamically include volunteers, experts, etc., in the operation as they see fit. A MANET for first responders is also likely to be used to distribute sensitive data (e.g. health records) among the participants, and therefore require some level of encryption. However, in a crisis situation the main objective is to save lives, making availability and integrity of the data more important than confidentiality.

For any tactical operation it is vital that commanding nodes (e.g. squad leader) have access to a situation map with the current layout of the network (optionally with geographical position). This coupled with the need for low latency in route discovery makes proactive protocols seem as a better choice than reactive ones.

3.2. Optimised Link State Routing Protocol

The Optimised Link State Routing (OLSR) protocol [4], [16] is a proactive protocol designed for MANETs. The protocol introduces the concept of Multi-Point Relay (MPR) flooding, where only designated nodes rebroadcast messages. Each node selects a subset of its neighbours, called the MPR set, such that every two-hop neighbour can be reached through at least one MPR. By restricting forwarding to only the nodes that have been selected MPR by the originator, the MPR scheme allows for an optimised packet flooding that greatly reduces the number of broadcasts compared to the general purpose flooding.

The protocol defines HELLO messages for local link sensing and Topology Change (TC) messages for network wide topology diffusion. Nodes advertise their link set and MPR selection through periodic broadcasts of HELLO messages

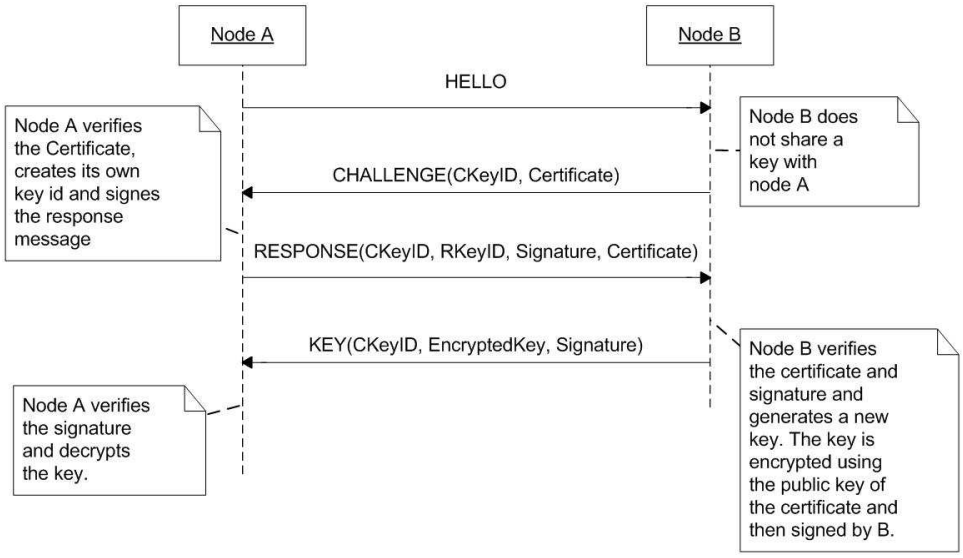

Figure 1. Key establishment process

containing all direct links with corresponding status (e.g. symmetric, MPR, etc). At the receiving end, the messages are used for link sensing, determine forwarding actions (whether the node is MPR or not) and to build two-hop neighbour topology that forms the basis for MPR selection. The node also maintain a MPR Selector Set containing all neighbours that have selected the node as MPR. HELLO messages are intended for neighbours only and are never forwarded.

Topology Change (TC) messages are periodically flooded in the network to allow nodes to build a complete routing table. The protocol requires that every node having been selected MPR must broadcast TC messages containing at least all neighbours in the MPR Selector Set. This being a minimum, additional links may be advertised for redundancy.

3.3. PKI

The authentication mechanism of our protocol is based on X.509 certificates [8] and requires the establishment of a certification authority (CA) for each organisation participating in the network. The CA operates off-line, i.e. does not participate in the MANET, and is responsible for issuing certificates to all its nodes. The number of hierarchical levels and their structure (geographical, organisational, etc) is configurable by the user. However, if two nodes that do not share a CA (at some level) are to authenticate each other, at least one of the certificates in the certificate chain must be cross signed, so that they may verify the authenticity of each others' certificate. For first responder organisations that are likely to cooperate, such cross-certification is recommended. The certificates must include an X.509 extension containing a description of the node and the certificate.

Distribution of Certificate Revocation Lists (CRLs) is not trivial, especially when allowing cross signed certificate authorities. In order to limit the size of CRLs and also the impact of failing to distribute CRLs, we propose to limit the validity time of certificates to typically a few months. The process may be automated as part of docking/re-charging procedure at the node's home location (e.g. at the hospital). CAs could have considerably longer validity time (e.g. years) since these are not exposed in the same way as mobile nodes.

In order to provide network access to nodes that do not possess regular first responder certificates, we propose a special short-term certificate. This type of certificate is issued on scene by regular authorised nodes. Whether all regular nodes, or only a subset of such (e.g. high ranking officers) are authorised to issue short-term certificates is configurable. With validity time set to 24 hours, the need for CRLs is diminished.

3.4. Authentication, key establishment and access control

In order to verify the authenticity of certificates (i.e. prove ownership), a challenge-response protocol is proposed. The process (depicted in Figure 1) is initiated whenever a new link is discovered (through the reception of a HELLO message) and consists of four main steps;

1) Node B generates a challenge (CKeyID[2]) for node A.
2) Node A signs the challenge (CKeyID) and generates a new one (RKeyID) for node B.

2. The challenges are later used as key identifier, hence the names

3) Node B verifies the response from A and generates a key.
4) Node A verifies the response from B and stores the received key.

This process serves three main functions as it 1) provides mutual authentication, 2) distribute the authorised node description (contained in the certificate), and 3) establishes a shared secret key.

After a successful authentication, the access control mechanism utilises the node description contained in the certificate extension to determine the access level to grant the node. We have defined two levels; where one is granted to all nodes with regular certificates, while the other is granted to nodes with temporary short-term certificates. The latter group is not allowed to be selected MPR and may therefore not interfere in routing protocol updates (except from the ones originating from the node itself).

3.5. Link encryption

We propose an effective symmetric encryption scheme where messages are encrypted on a per link basis. The scheme relies on the establishment of symmetric keys for each pair of neighbours. These keys are denoted *link keys* and established during the final step of the authentication and key establishment process described previously.

To reduce the processing overhead for intermediate nodes, the payload is encrypted once using a one-time key, whereas the one-time key is encrypted using the link key. Thus, intermediate forwarding nodes need only decrypt and re-encrypt the header field, rather than the entire packet. Additionally, to accommodate broadcast messages, multiple headers are allowed such that all neighbouring nodes may decrypt the one-time key using their link key. This way one need not repeat the entire payload, only the minimal header.

4. Protocol description

Our protocol description is based on the OLSR protocol and is aimed at pointing out where the two protocols differ. Hence, we will often refer to the OLSR specification (RFC 3626 [4]) on matters that are not treated specifically by our security extension.

4.1. Message formats and processing

All existing OLSR messages such as TC and HELLO messages are distributed in broadcast mode without explicit addresses of recipients. For our link encryption scheme we therefore define the general encrypted message format (Figure 2) to allow multiple recipients of the per link encrypted message. The summary section contains the number of key blocks (`KB_counter`) and the type and length of the Message Authentication Code (MAC) (`MAC_length`). There is one Key Block for each recipient containing a key identifier (`Key_id`) and the one-time key encrypted with the corresponding key. The MAC and encrypted payload constitutes the rest of the message. By using key identifiers instead of IP addresses, the protocol does not allow adversaries to eavesdrop on the communication in order to get an overview

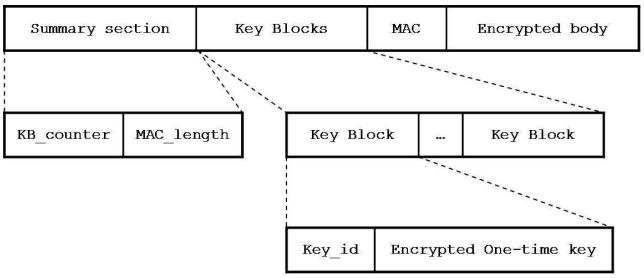

Figure 2. General encrypted message format encapsulating HELLO and TC messages

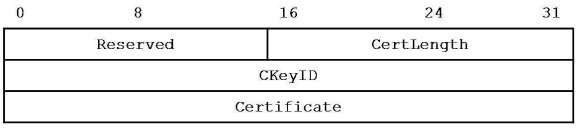

Figure 3. Challenge message format

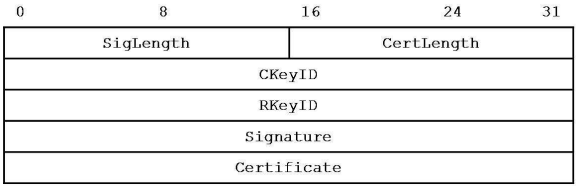

Figure 4. Response message format

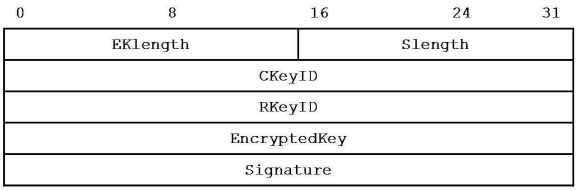

Figure 5. KEY message format

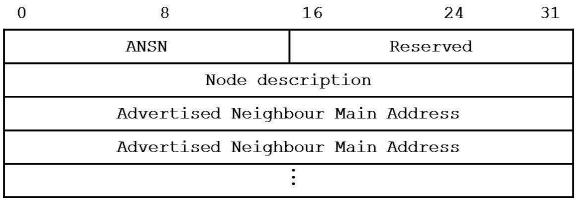

Figure 6. TC message format after decryption

of participating nodes.

The encrypted HELLO message defined for our protocol is identical to the original HELLO message format after decryption. The encrypted TC messages contain a node description in addition to the already specified solution (see Figure 6).

The message formats for our challenge response protocol are given in Figure 3,4 and 5. The key identifiers (`CKeyID/RKeyID`) are selected randomly and therefore also serve as nonces.

4.2. Information bases

We extend the information bases for OLSR to include link keys, node descriptions and access level. The link set tuple is extended to include local and neighbour key identifiers (`L_local_KID`,`L_neighbour_KID`) and key value (`L_key_value`). The local key identifier is used whenever a message is sent to a node, while the neighbour key identifier is used whenever a message is received. Local key identifiers must be unique for each node, while neighbour key identifiers need not. The neighbourhood information base is extended to include the authenticated node description extracted from the certificate during key establishment.

The topology information base is extended with a new Node Description Set, where each tuple contain a node address (`ND_main_address`) and the corresponding node description (`ND_node_description`).

4.3. Link sensing

Due to our link encryption scheme, the process of link sensing and neighbour discovery is slightly different from the OLSR protocol. In OLSR, link sensing and neighbour discovery is performed through periodical HELLO message transmissions, containing known links to one-hop neighbours. However, our link encryption scheme requires the establishment of a shared secret key prior to any regular message processing. The process is initiated whenever a HELLO message is received and the sender and receiver do not share a key. After decryption, HELLO messages are processed in the same way as the original OLSR protocol, with some minor changes.

The interpretation of link codes is slightly changed from the original OLSR protocol. We regard a link to be symmetric (`SYM_LINK`) only if the nodes share a symmetric link and a key has been established. If the link has been detected but no key has been established, the link is considered asymmetric (`ASYM_LINK`). We also define a new neighbour type for the situation where the link is symmetric and the the node has only restricted access to the network (`RES_SYM_NEIGH`). Only nodes that have no access restrictions are eligible to be selected MPR and hence to take part in routing control message forwarding.

4.4. Topology discovery

To discover nodes and links outside the 2-hop neighbourhood all nodes distribute Topology Control (TC) messages containing their advertised neighbour set and node description (see Figure 6). Similar to the HELLO message, TC messages are also encapsulated in the general encrypted message format (Figure 2) and broadcast to all neighbouring nodes with which the nodes share a symmetric link.

The node description is only authenticated to immediate neighbours (during key establishment) and not within the TC message. While such authentication is desirable, it would severely increase the control data overhead and possibly exhaust bandwidth resources. Therefore, whenever a TC message is received from a neighbour, the node verifies that the node description contained in the TC message is identical to the authenticated description received during key establishment. In the event of a mismatch, the TC message is silently discarded. After decrypting the TC message, it is processed according to the original OLSR protocol. If the message is considered valid (i.e. not processed before) the node description set is updated with the new description found in the TC message.

4.5. Routing table calculation

The routing table calculation is performed in the same manner as the OLSR protocol, with one slight difference resulting from the split network architecture described in section 3.4, where only nodes with no access restrictions are allowed to forward packets. The routing table calculation must take this into account in order to avoid paths containing limited access nodes.

Thus, in order to compute the routing table for node X, a shortest path algorithm is run on the directed graph containing:

1) The neighbour arcs $X \rightarrow Y$, where Y is a symmetric neighbour of X.
2) The 2-hop neighbour arcs $Y \rightarrow Z$, where Y is a neighbour node with willingness different of `WILL_NEVER` and Y's node description specifies no access restrictions and Y, Z belongs to the 2-hop neighbour set.
3) The topology arcs $U \rightarrow V$, where there exist an entry in the topology set with V as `T_dest_addr` and U as `T_last_addr` and U's node description specifies no access restrictions.

5. Discussion

Our link encryption scheme does not provide end to end security since intermediate nodes are able to decrypt, and possibly change the content of the message, without the receiver noticing. However, the distribution of routing information is mainly done by broadcasting messages, which

makes end to end confidentiality meaningless. To allow for end to end message authentication would require either the full distribution of certificates (periodically) or dynamic establishment of symmetric keys between all nodes in the network. In either case, the resource consumption is significant and also scalability issues would arise as the number of nodes in the network increases. Another possibility would be to have all nodes share a single network wide symmetric key. However, this approach makes key management and key agreement a particularly demanding task. Key renewal may then render the network inoperable for a period of time (until the new key is fully distributed), which is considered unacceptable for emergency and rescue operations.

There is considerable risk involved in admitting non-first responders to the network through temporary access. However, by restricting the participation so as to not interfere with the routing protocol operation, the associated risk is greatly reduced. It is also assumed that dynamically granting of access is required in order to take full advantage of the MANET potential.

6. Conclusion and further work

We have presented a secure ad hoc network scheme for first responders in a crisis situation that provides access control and confidentiality of information. This scheme balances the need for protection with requirements for availability and efficiency, and takes advantage of the hierarchical structure of such operations.

In the next phase we will perform simulations of our solution using NS2. We will also extend our model to enable a more efficient secure multi-cast or group communication scheme that can provide confidentiality from non-members.

Acknowledgements

This paper has presented results from the EU FP6 OASIS research project, with additional funding by the Norwegian Research Council. Thanks to Ingrid S. Svagård for making this possible.

References

[1] A. Meissner, T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner, "Design challenges for an integrated disaster management communication and information system," in *The First IEEE Workshop on Disaster Recovery Networks (DIREN 2002)*, vol. 24, 2002.

[2] "Oasis project web page." [Online]. Available: http://www.oasis-fp6.org

[3] N. Andrienko and G. Andrienko, "Intelligent visualisation and information presentation for civil crisis management," *Transactions in GIS*, vol. 11, no. 6, pp. 889–909, 2007.

[4] T. Clausen and P. Jacquet, Eds., *RFC3626: Optimized Link State Routing Protocol (OLSR)*. IETF, The Internet Society, Oct. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[5] C. E. Perkins, E. M. Belding-Royer, and S. Das, *RFC3561: Ad hoc On-Demand Distance Vector (AODV) Routing*. IETF, The Internet Society, Jul. 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[6] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, ser. Signals and Communication Technology. Springer US, 2007, pp. 103–135.

[7] L. Venkatraman and D. P. Agrawal, "Strategies for enhancing routing security in protocols for mobile ad hoc networks," *Journal of Parallel and Distributed Computing*, vol. 63, pp. 214–227, Feb. 2003.

[8] D. Cooper, Santesson, Farrell, Boeyen, R. Housley, and W. Polk, *RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF, The Internet Society, May 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5280.txt

[9] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated routing for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 23, pp. 598–610, 2005.

[10] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM workshop on Wireless security*. Atlanta, GA, USA: ACM, 2002, pp. 1–10.

[11] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*. IEEE Computer Society, 2003, p. 379.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wirel. Netw.*, vol. 11, no. 1-2, pp. 21–38, 2005.

[13] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," *in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002*, pp. 27–31, 2002.

[14] P. Papadimitratos and Z. Haas, "Secure data communication in mobile ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 343–356, 2006.

[15] M. Puzar, T. Plagemann, and Y. Roudier, "Security and privacy issues in middleware for emergency and rescue applications," *Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on*, pp. 89–92, 30 2008-Feb. 1 2008.

[16] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International*, 2001, pp. 62–68.